Oracle Cloud Infrastrucure（OCI）上の Cisco ISE

Oracle Cloud Infrastrucure（OCI）上の Cisco ISE

Cisco ISE は Oracle Cloud Infrastructure（OCI）で使用できます。OCI で Cisco ISE を設定してインストールするには、OCI のいくつかの機能とソリューションについてよく理解しておく必要があります。開始する前に理解しておく必要がある概念には、コンパートメント、可用性ドメイン、イメージとシェイプ、ブートボリュームなどがあります。OCI のコンピューティングリソースの単位は、Oracle CPU（OCPU）です。1 つの OCPU は、2 つの vCPU に相当します。

『Oracle Cloud Infrastructure Documentation』を参照してください。

Cisco ISE は、イメージとスタックの 2 つの形式で OCI で利用できます。Cisco ISE ユーザーが使いやすいようにカスタマイズされていることから、スタックタイプを使用して Cisco ISE をインストールすることをお勧めします。

- Terraform スタックファイルを使用した OCI での Cisco ISE インスタンスの作成 （6 ページ）
- OCI での Cisco ISE インスタンスの作成 （4 ページ）

Oracle Cloud Infrastrucure（OCI）上の Cisco ISE

表 *1 : Cisco ISE* でサポートされる *OCI* インスタンス

OCI インスタンス	OCPU	OCI インスタンスメモリ（GB 単位）
Standard3.Flex （このインスタンスは、Cisco ISE 評価のユースケースをサポートしています。100 の同時アクティブエンドポイントがサポートされています）	2	16
Optimized3.Flex	8	32
	16	64
Standard3.Flex	4	32
	8	64
	16	128
	32	256

Optimized3.Flex シェイプはコンピューティングに最適化され、コンピューティング集約型のタスクやアプリケーションの PSN として使用するのに最適です。

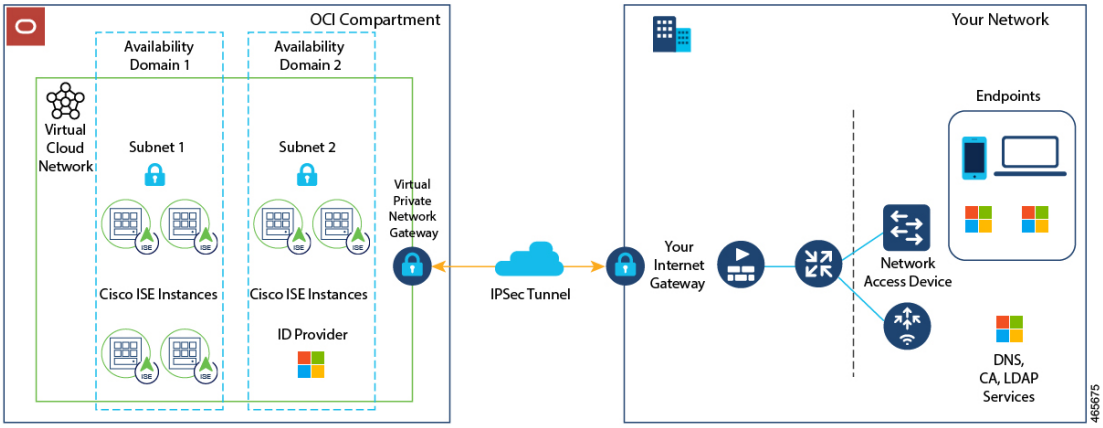
Standard3.Flex シェイプは、PAN または MnT ノード、またはその両方としての使用に最適な汎用のシェイプであり、データ処理タスクとデータベース操作を目的としています。

汎用インスタンスを PSN として使用する場合、パフォーマンスの数値は、PSN としてのコンピューティング最適化インスタンスのパフォーマンスよりも低くなります。

Standard3.Flex（4 OCPU、32 GB）シェイプは、極小規模の PSN としてのみ使用する必要があります。

OCI インスタンスタイプのスケールおよびパフォーマンスデータについては、『Performance and Scalability Guide for Cisco Identity Services Engine』を参照してください。

図 *1 : Oracle Cloud* に接続された展開の例



（注） Cisco ISE インスタンスを作成するために既存の OCI イメージを複製しないでください。

OCI 上の Cisco ISE の使用に関する既知の制限事項

- Cisco ISE アップグレードワークフローは、OCI 上の Cisco ISE では使用できません。新規インストールのみがサポートされています。ただし、設定データのバックアップと復元は実行できます。
- パブリッククラウドはレイヤ 3 機能のみをサポートします。OCI 上の Cisco ISE ノードは、レイヤ 2 の機能に依存する Cisco ISE 機能をサポートしません。たとえば、Cisco ISE CLI を介した DHCP SPAN プロファイラプローブおよび CDP プロトコル機能の使用は、現在サポートされていない機能です。
- Cisco ISE で IPv6 アドレスを有効にするには、Cisco ISE の OCI ポータルで IPv6 アドレスを設定し、インターフェイス ギガビット イーサネット 0 を再起動します。Cisco ISE シリアルコンソールに管理者としてログインし、次のコマンドを実行します。

```
#configure terminal
Entering configuration mode terminal
(config)#interface GigabitEthernet 0
(config-GigabitEthernet-0)#shutdown
(config-GigabitEthernet-0)#no shutdown
(config-GigabitEthernet-0)#exit
(config)#exit
```

- 設定データの復元およびバックアップ機能を実行する場合、バックアップ操作が完了した後、まず CLI から Cisco ISE を再起動します。次に、Cisco ISE GUI から復元操作を開始します。Cisco ISE のバックアップおよび復元プロセスの詳細については、お使いのバージョンのリリースの『Cisco ISE Administrator Guide』の「Maintain and Monitor」の章を参照してください。
- パスワードベースの認証を使用した Cisco ISE CLI への SSH アクセスは、OCI ではサポートされていません。キーペアを介してのみ Cisco ISE CLI にアクセスできます。このキーペアを安全に保管してください。

  秘密キー（または PEM）ファイルを使用していてそのファイルを失った場合、Cisco ISE CLI にアクセスできません。

  パスワードベースの認証方式を使用して Cisco ISE CLI にアクセスする統合は、サポートされていません（たとえば、Cisco DNA Center リリース 2.1.2 以前）。

OCI での Cisco ISE インスタンスの作成

始める前に

- 次のタスクの手順3を開始する前に、コンパートメント、カスタムイメージ、シェイプ、仮想クラウドネットワーク、サブネット、およびサイト間 VPN を作成します。

  Cisco ISEインスタンスを作成するのと同じコンパートメントに仮想クラウドネットワークとサブネットを作成します。

- Cisco ISE で使用する仮想クラウドネットワークを作成するときは、[インターネット接続を使用してVCNを作成（Create VCN with Internet Connectivity）] VCN タイプを選択することをお勧めします。

ステップ 1 OCI アカウントにログインします。

ステップ 2 検索フィールドを使用して、**マーケットプレイス**を検索します。

ステップ 3 [リストの検索（Search for listings...）] の検索フィールドで、**Cisco Identity Services Engine（ISE）**と入力します。

ステップ 4 **イメージ**タイプの Cisco ISE オプションをクリックします。

ステップ 5 表示される新しいウィンドウで、[インスタンスの起動（Launch Instances）] をクリックします。

ステップ 6 左ペインの [リストスコープ（List Scope）] エリアで、[コンパートメント（Compartment）] ドロップダウンリストからコンパートメントを選択します。

ステップ 7 右ペインで [インスタンスの作成（Create Instance）] をクリックします。

ステップ 8 表示される [コンピューティングインスタンスの作成（Create Compute Instance）] ウィンドウの [名前（Name）] フィールドに、Cisco ISE インスタンスの名前を入力します。

ステップ 9 [コンパートメントに作成（Create in Compartment）] ドロップダウンリストから、Cisco ISE インスタンスを作成する必要があるコンパートメントを選択します。Cisco ISE で使用する仮想クラウドネットワークやサブネットなどの他のリソースを作成したコンパートメントを選択する必要があります。

ステップ 10 [配置（Placement）]エリアで可用性ドメインをクリックします。ドメインによって利用可能なコンピューティングシェイプが決められます。

ステップ 11 [イメージとシェイプ（Image and Shape）] エリアで次の手順を実行します。

a) [イメージの変更（Change Image）] をクリックします。
b) [イメージソース（Image Source）] ドロップダウンリストから、[カスタムイメージ（Custom Image）] を選択します。
c) 必要なカスタムイメージ名の横にあるチェックボックスをオンにします。
d) [イメージの選択（Select Image）] をクリックします。
e) [イメージとシェイプ（Image and Shape）] エリアから、[シェイプの変更（Change Shape）] をクリックします。
f) [シェイプシリーズ（Shape Series）]エリアから、[Intel] をクリックします。使用可能なシェイプのリストが表示されます。

g) 必要なシェイプ名の横にあるチェックボックスをオンにします。[シェイプの選択（Select Shape）] をクリックします。

ステップ 12 [ネットワーク（Networking）] エリアで次の手順を実行します。

a) [プライマリネットワーク（Primary Network）] エリアで、[既存の仮想クラウドネットワークを選択（Select existing virtual cloud network）] オプションボタンをクリックします。

b) ドロップダウンリストから仮想クラウドネットワークを選択します。

c) [サブネット（Subnet）] エリアで、[既存のサブネットを選択（Select existing subnet）] オプションボタンをクリックします。

d) ドロップダウン リストからサブネットを選択します。表示されるサブネットは、同じコンパートメントで作成されたサブネットです。

ステップ 13 [SSHキーの追加（Add SSH Keys）] エリアで、対応するオプションボタンをクリックして、キーペアを生成するか、既存の公開キーを使用できます。

ステップ 14 [ブートボリューム（Boot Volume）]エリアで、[カスタムブートボリュームサイズの指定（Specify a custom boot volume size）] チェックボックスをオンにして、必要なブートボリュームを GB 単位で入力します。Cisco ISE 実稼働環境に必要な最小ボリュームは 600 GB です。この手順でブートボリュームが指定されていない場合、インスタンスに割り当てられるデフォルトのボリュームは 250 GB です。

ステップ 15 [詳細オプションの表示（Show advanced options）] をクリックします。

ステップ 16 [管理（Management）] タブで、[クラウド初期化スクリプトの貼り付け（Paste cloud-init script）] オプションボタンをクリックします。

ステップ 17 表示される [クラウド初期化スクリプト（Cloud-init script）] テキストボックスを使用して、必要なユーザーデータを入力します。

[ユーザーデータ（User data）] フィールドに次の情報を入力します。

hostname=<*hostname of Cisco ISE*>

primarynameserver=<*IPv4 address*>

dnsdomain=<*example.com*>

ntpserver=<*IPv4 address or FQDN of the NTP server*>

timezone=<*timezone*>

password=<*password*>

ersapi=<*yes/no*>

openapi=<*yes/no*>

pxGrid=<*yes/no*>

pxgrid_cloud=<*yes/no*>

ユーザーデータエントリを使用して設定する各フィールドには、正しいシンタックスを使用する必要があります。[ユーザーデータ（User Data）] フィールドに入力した情報は、入力時に検証されません。誤った構文を使用すると、イメージの起動時に Cisco ISE サービスが表示されないことがあります。次に、[ユーザーデータ（User Data）] フィールドを使用して送信する設定のガイドラインを示します。

- hostname：英数字とハイフン（-）のみを含むホスト名を入力します。ホスト名の長さは 19 文字以下で、下線（_）を含めることはできません。

- プライマリネームサーバー：プライマリネームサーバーの IP アドレス。サポートされているのは IPv4 アドレスだけです。
- dnsdomain：DNS ドメインの FQDN を入力します。エントリには、ASCII 文字、数字、ハイフン（-）、およびピリオド（.）を含めることができます。
- ntpserver：同期に使用する NTP サーバーの IPv4 アドレスまたは FQDN を入力します（例：time.nist.gov）。
- timezone：タイムゾーンを入力します（例：Etc/UTC）。すべての Cisco ISE ノードを協定世界時（UTC）のタイムゾーンに設定することを推奨します（特に Cisco ISE ノードが分散展開されてインストールされている場合）。これにより、展開内のさまざまなノードからのレポートとログのタイムスタンプが常に同期されます。
- password：Cisco ISE への GUI ベースのログインのパスワードを設定します。入力するパスワードは、Cisco ISE のパスワードポリシーに準拠している必要があります。たとえば、パスワードには、少なくとも 1 つの小文字、1 つの大文字、および 1 つの数字を含む 8 文字以上が含まれている必要があります。パスワードには、admin、cisco、password などの特定のディクショナリエントリを含めることはできません。ご使用のリリースの『Cisco ISE Administrator Guide』[英語] の「Basic Setup」の章にある「User Password Policy」のセクションを参照してください。
- ersapi：ERS を有効にするには **yes** と入力し、ERS を拒否するには **no** と入力します。
- openapi：OpenAPI を有効にするには **yes** と入力し、OpenAPI を拒否するには **no** と入力します。
- pxGrid：pxGrid を有効にするには **yes** と入力し、pxGrid を拒否するには **no** と入力します。
- pxgrid_cloud：pxGrid Cloud を有効にするには **yes** と入力し、pxGrid Cloud を拒否するには **no** と入力します。pxGrid クラウドを有効にするには、pxGrid を有効にする必要があります。pxGrid を無効にして pxGrid クラウドを有効にすると、pxGrid クラウドサービスは起動時に有効になりません。

ステップ 18 [作成（Create）] をクリックします。インスタンスが作成されて使用できるようになるまで、約 30 分かかります。

Cisco ISE インスタンスを表示するには、[インスタンス（Instances）] ウィンドウに移動します（検索フィールドを使用してウィンドウを見つけることができます）。Cisco ISE インスタンスがこのウィンドウにリストされます。

Terraform スタックファイルを使用した OCI での Cisco ISE インスタンスの作成

始める前に

OCI Terraform を利用して、Cisco ISE インスタンスを作成します。OCI の Terraform については、https://docs.oracle.com/en-us/iaas/Content/API/SDKDocs/terraform.htm を参照してください。

OCI で、SSH キー、仮想クラウドネットワーク（VCN）、サブネット、ネットワーク セキュリティ グループなど、Cisco ISE インスタンスを作成するために必要なリソースを作成します。

ステップ 1 OCI アカウントにログインします。

ステップ 2 検索フィールドを使用して、**マーケットプレイス**を検索します。

ステップ 3 [リストの検索（Search for listings...）] の検索フィールドで、**Cisco Identity Services Engine（ISE）**と入力します。

ステップ 4 [Cisco Identity Services Engine（ISE）スタック（Cisco Identity Services Engine (ISE) Stack）] をクリックします。

ステップ 5 表示される新しいウィンドウで、[スタックの作成（Create Stack）] をクリックします。

ステップ 6 [スタック情報（Stack Information）] ウィンドウで次の手順を実行します。

a) [マイ設定（My Configuration）] オプションボタンをクリックします。

b) [コンパートメントに作成（Create in Compartment）] ドロップダウンリストから、Cisco ISE インスタンスを作成するコンパートメントを選択します。

ステップ 7 **[Next]** をクリックします。

ステップ 8 [変数の構成（Configure Variables）] ウィンドウで、次の手順を実行します。

a) [ホスト名（Hostname）] フィールドに、ホスト名を入力します。

b) [シェイプ（Shape）] ドロップダウンリストから、使用する OCI シェイプを選択します。[VM.Optimized3.Flex] を選択した場合は、[Flex OCPU] ドロップダウンリストから必要な値を選択します。[Flexメモリ（GB）（Flex Memory in GB）] フィールドには、対応する値が自動的に表示されます。他のシェイプでは値は事前に設定され、これらのフィールドはスタック形式に表示されません。

c) [ブートボリュームサイズ（Boot Volume Size）] フィールドには、前の手順で選択したシェイプに基づいて必要な値が自動的に表示されます。

d) [SSHキー（SSH Key）] エリアで、対応するオプションボタンをクリックして、SSH キーファイルをアップロードするか、SSH キーコードを貼り付けることができます。

e) [タイムゾーン（Time Zone）] ドロップダウンリストから、タイムゾーンを選択します。

f) [可用性ドメイン（Availability Domain）] ドロップダウンリストで、リージョンのドメインのリストからオプションを選択します。

g) [仮想クラウドネットワーク（Virtual Cloud Network）] ドロップダウンリストで、手順 6b で選択したコンパートメントの VCN のリストからオプションを選択します。

h) [サブネット（Subnet）] ドロップダウンリストで、手順 8g で選択した VCN に関連付けられたサブネットのリストからオプションを選択します。

i) （任意）[ネットワークセキュリティグループ（Network Security Group）] ドロップダウンリストで、前に選択したコンポーネントに関連付けられているセキュリティグループのリストからオプションを選択します。

j) [パブリックIPアドレスの割り当て（Assign Public IP Address）] チェックボックスはデフォルトでオンになっています。Cisco ISE インスタンスにプライベート IP アドレスのみを割り当てる場合は、チェックボックスをオフにすることができます。

k) [プライベートIPアドレス（Private IP Address）] フィールドに、選択したサブネットで定義されている IP アドレス範囲に準拠する IP アドレスを入力します。このフィールドを空白のままにすると、OCI DHCP サーバーが Cisco ISE に IP アドレスを割り当てます。

l) [DNS名（DNS Name）] フィールドにドメイン名を入力します。

m) [ネームサーバー（Name Server）] フィールドに、ネームサーバーの IP アドレスを入力します。この IP アドレスが誤った構文を使用している、または到達できない場合、Cisco ISE サービスが起動時に表示されないことがあります。

n) [NTPサーバー（NTP Server）] フィールドに、NTP サーバーの IP アドレスまたはホスト名を入力します。エントリは入力時に検証されません。IP アドレスが正しくない場合、Cisco ISE サービスが起動時に表示されないことがあります。

o) [ERS] ドロップダウンリストから、[はい（Yes）] または [いいえ（No）] を選択します。

p) [オープンAPI（Open API）] ドロップダウンリストから、[はい（Yes）] または [いいえ（No）] を選択します。

q) [pxGrid] ドロップダウンリストから、[はい（Yes）] または [いいえ（No）] を選択します。

r) [pxGridクラウド（pxGrid Cloud）] ドロップダウンリストから、[はい（Yes）] または [いいえ（No）] を選択します。

a) [パスワード（Password）] および [パスワードの再入力（Re-enter Password）] フィールドに Cisco ISE のパスワードを入力します。パスワードは Cisco ISE のパスワードポリシーに準拠し、最大 25 文字である必要があります。

ステップ 9 **[Next]** をクリックします。

[レビュー（Review）] ウィンドウに、スタックで定義されているすべての設定の概要が表示されます。

ステップ 10 情報を確認し、変更がある場合は [前へ（Previous）] をクリックして変更します。

ステップ 11 [作成したスタックで適用を実行（Run Apply on the created stack?）] エリアで、[適用を実行（Run Apply）] チェックボックスをオンにすると、[作成（Create）] をクリックしたときにスタックビルドが実行されます。[適用を実行（Run Apply）] を選択していない場合、[作成（Create）] をクリックしたときにスタック情報が保存されます。後で [スタック（Stacks）] ウィンドウからスタックを選択し、[適用（Apply）] をクリックしてビルドを実行できます。

ステップ 12 [作成（Create）] をクリックします。

ステップ 13 OCI の [インスタンス（Instances）] ウィンドウに移動します。インスタンスは、スタック形式で指定したホスト名とともにリストされます。ホスト名をクリックすると、設定の詳細が表示されます。

ステップ 14 Cisco ISE インスタンスは、約 30 分で OCI で起動できるようになります。

インストール後のタスク

Cisco ISE インスタンスを正常に作成した後に実行する必要があるインストール後のタスクについては、お使いのバージョンの Cisco ISE リリースの『Cisco ISE Installation Guide』の「Installation Verification and Post-Installation Tasks」の章を参照してください。

OCI 上の Cisco ISE の互換性情報

このセクションでは、OCI 上の Cisco ISE に固有の互換性情報について詳しく説明します。Cisco ISE の一般的な互換性の詳細については、お使いのバージョンのリリースの『Cisco Identity Services Engine Network Component Compatibility』ガイドを参照してください。

ロードバランサ統合のサポート

RADIUS トラフィックのロードバランシングのために、OCI ネイティブ ネットワーク ロード バランサ（NLB）を Cisco ISE と統合できます。ただし、次の注意事項が適用されます。

- 認可変更（CoA）機能は、ネットワークロードバランサを作成するときに、送信元や宛先のヘッダー（IP、ポート）の保存セクションでクライアント IP の保存を有効にしている場合にのみサポートされます。
- NLB は送信元 IP アフィニティのみをサポートし、発信側ステーション ID ベースのスティッキセッションをサポートしないため、不均等なロードバランシングが発生する可能性があります。
- NLB は RADIUS ベースのヘルスチェックをサポートしていないため、RADIUS サービスがノードでアクティブでない場合でも、トラフィックを Cisco ISE PSN に送信できます。

OCI ネイティブ ネットワーク ロードバランサの詳細については、『Introduction to Network Load Balancer』を参照してください。

TACACS トラフィックのロードバランシングのために、OCI ネイティブ ネットワーク ロード バランサ（NLB）を Cisco ISE と統合できます。ただし、NLB は TACACS+ サービスに基づくヘルスチェックをサポートしないため、ノードで TACACS サービスがアクティブでない場合でも、Cisco ISE PSN にトラフィックが送信されることがあります。

NIC ジャンボフレームサポート

Cisco ISE はジャンボフレームをサポートしています。Cisco ISE の最大伝送ユニット（MTU）は 9,001 バイトですが、ネットワーク アクセス デバイスの MTU は通常 1,500 バイトです。Cisco ISE は、標準フレームとジャンボフレームの両方を問題なくサポートし、受信します。コンフィギュレーション モードで Cisco ISE CLI を使用して、Cisco ISE MTU を必要に応じて再設定できます。

OCI でのパスワードの回復とリセット

次のタスクでは、Cisco ISE 仮想マシンのパスワードをリセットするために役立つタスクについて説明します。必要なタスクを選択し、詳細な手順を実行します。

シリアルコンソールを介した Cisco ISE GUI パスワードのリセット

ステップ 1 OCI にログインし、[コンピューティング（Compute）] の [インスタンス（Instances）] ウィンドウに移動します。

ステップ 2 インスタンスのリストから、パスワードを変更する必要があるインスタンスをクリックします。

ステップ 3 左ペインの [リソース（Resource）] メニューから、[コンソール接続（Console connection）] をクリックします。

ステップ 4 [Cloud Shell接続の起動（Launch Cloud Shell connection）] をクリックします。

ステップ 5 新しい画面に Oracle Cloud Shell が表示されます。

ステップ 6 画面が黒い場合は、Enter を押してログインプロンプトを表示します。

ステップ 7 シリアルコンソールにログインします。

シリアルコンソールにログインするには、インスタンスのインストール時に設定された元のパスワードを使用する必要があります。OCI は、この値をマスクされたパスワードとして保存します。このパスワードを覚えていない場合は、「パスワードの回復」セクションを参照してください。

ステップ 8 **application reset-passwd ise iseadmin** コマンドを使用して、iseadmin アカウントの新しい Cisco ISE GUI パスワードを設定します。

新しい公開キーペアの作成

このタスクを通じて、追加のキーペアをリポジトリに追加します。Cisco ISE インスタンスの設定時に作成された既存のキーペアは、新しく作成する公開キーに置き換えられません。

ステップ 1 OCI で新しい公開キーを作成します。『Creating a Key Pair』を参照してください。

ステップ 2 前のタスクで説明したように、OCI シリアルコンソールにログインします。

ステップ 3 公開キーを保存する新しいリポジトリを作成するには、『Creating a Repository』を参照してください。

CLI を介してアクセスできるリポジトリがすでにある場合は、手順 4 に進みます。

ステップ 4 新しい公開キーをインポートするには、コマンド **crypto key import <public key filename> repository <repository name>** を使用します。

ステップ 5 インポートが完了すると、新しい公開キーを使用して SSH 経由で Cisco ISE にログインできます。

パスワードの回復

OCI には Cisco ISE のパスワード回復のメカニズムはありません。新しい Cisco ISE インスタンスを作成し、設定データのバックアップと復元を実行する必要が生じる場合があります。

OCI スタックの変数を編集すると、設定や構成を保存せずに Cisco ISE インスタンスが破棄され、新しい Cisco ISE インスタンスとして再作成されます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。